UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/990,842	11/21/2001	Paul A. Moskowitz	CHA920010021US1	2704

45095 7590 04/30/2009

HOFFMAN WARNICK LLC
75 STATE ST
14 FL
ALBANY, NY 12207

EXAMINER	
NELSON, FREDA ANN	

ART UNIT	PAPER NUMBER
3628	

NOTIFICATION DATE	DELIVERY MODE
04/30/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOCommunications@hoffmanwarnick.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/990,842
Filing Date: November 21, 2001
Appellant(s): MOSKOWITZ ET AL.

Carl F. Ruoff
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed January 28, 2009 appealing from the Office action mailed January 18, 2009.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,230,081	ALBERTSHOFER	05-2001
5,914,471	VAN DE PAVERT	06-1999
5,955,970	FORCE ET AL.	07-1996
5,844,986	DAVIS	12-1998
US 2003/0009683	SCHWENCK ET AL.	01-2003

US 2001/0039509	DAR ET AL.	11-2001
US 2001/0037298	EHRMAN ET AL.	11-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-2, 8, 12-14, 33 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albertshofer (US Patent Number 6,230,081), in view of Van De Pavert (Patent Number 5,914,471).

As per claims 1, 8, 12, and 33, Albertshofer discloses a sensor for gathering usage data from the remote apparatus (col. 3, lines 31-39; col. 5, lines 10-15; see claim 12); and

a processor for processing the gathered usage data and calculating a charge based on the gathered usage data (col. 5, lines 10-14; col. 5, lines 43-52; col. 6, lines 14-16; col. 6, lines 23-32; col. 1, line 29-39; abstract).

While Albertshofer discloses a control unit includes ***a means for encoding the usage data and the write means writes the usage data in encoded form to said chip card*** (see claim 1), Albertshofer does not explicitly disclose wherein a security system comprises an encryption system for encrypting usage data transmitted between the sensor and the processor.

However, Van De Pavert discloses ***cryptographically encoding said first authorization code*** (see claims 24 and 27). Van De Pavert further discloses an invention which relates to the secure storage of cost data in counters of public telephone sets of the type where a caller pays by means of a card, such as a so-called "chip" card and relates to recording usage data in general and cost data in particular for machines through which the purchaser pays by means of a card, such as, e.g., vending machines for sweets or for soft drinks, certain types of parking meters and stamp vending machines wherein the term "card" should be taken to refer to any type of card (or equivalent of a card) which enables the user to make use of the machine in question. Van De Pavert further disclose that here, the card advantageously and illustratively comprises a microprocessor 50 for processing data; memory 40 having a random access memory (RAM) 47 for temporarily storing data, such as usage data; and, optionally, cryptographic circuitry (54) for performing cryptographic operations, e.g., encryption and decryption (col. 15, line 2-18; FIG. 2 [1] is sensor and [2] is the processor; FIG. 3D [metering pulses]).

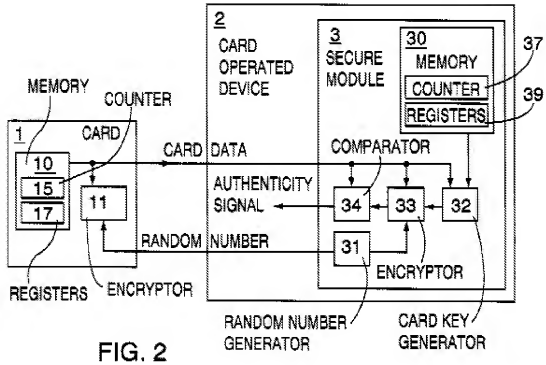

FIG. 2

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention Albertshofer to include the feature of Van De Pavert because it would have yielded predictable results. Further, applying the encryption system with sensors to Albertshofer would have been recognized by those of ordinary skill in the art as resulting in an improved system that would to provide enhanced security (Van De Pavert; col. 4, lines 37- 44).

As per claim 2, Albertshofer discloses a communications system for transmitting the calculated charge to a central server via a wireless transmission channel (col. 1, lines 40-48).

As per claim 13, Albertshofer discloses the system of claim 1, wherein the sensor measures a speed of the apparatus (col. 1, lines 55-61).

As per claim 14, Albertshofer discloses wherein the sensor collects data from a GPS system (col. 6, line 66-co1.7, line 2).

As per claim 36, Albertshofer discloses wherein the charge is a rental cost (col. 6, lines 23-280

2. Claims 3-5 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albertshofer (US Patent Number 6,230,081), in view of Van De Pavert (Patent Number 5,914,471), as applied to claims 1-2 above, and further in view of Ando et al. (Patent Number 5,955,970).

As per claims 3-5, Albertshofer disclose a security system claim 2, as described above, but does not disclose the security system comprising a tamper resistant encasement that encases at least one component of the local data processing system; wherein the encased component comprises the processor; and wherein the encased component comprises the sensor.

However, Ando et al. disclose that ***the on-board device must include a security system for protecting monetary data stored therein and ensuring legitimate communication with the stationary device*** (col. 1, lines 26-30). Ando et al.

further disclose that *the illegitimate opening of the on-line device can be detected by sensing the removal of crews fastening a circuit board to a case of the on-board* device. (col. 2, lines 7-9) The Examiner interprets this to mean a tamper resistant encasement). Ando et al. still further disclose that *the switch is connected to a processor of the on-board device to detect the removal of the screws* (col. 2, lines 11-13). Ando et al. further discloses that *Detectors 5 and 7 detect a vehicle and set a timing of communication between the on-board device and the stationary device. Gate entrance detector 9 and gate exit detector 10 set a timing of opening and closing the gate* (col. 3, lines 30-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Albertshofer to include the security system feature of Van De Pavert and Ando et al. in order to protect the monetary data stored therein the sensor (Ando et al.; col. 1, lines 26-30).

As per claim 15, Albertshofer does not expressly disclose that the sensor measures weight placed on the remote apparatus, however the Examiner takes Official Notice that it is old and well known that condition responsive indicating systems/sensors are sensitive to touch or weight placed on remote apparatuses, i.e. vehicles. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Albertshofer to include the sensor which measures weight in order to avoid intrusion.

3. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albertshofer (US Patent Number 6,230,081), in view of Van De Pavert (US Patent Number 5,914,471), still further view of Ando et al. (Patent Number 5,955,970), as applied to claim 3 above, and further in view of Force et al. (US Patent Number 5,533,123), in further view of Schwenck et al. (US PG Pub. 2003/0009683).

As per claim 6, Albertshofer does not disclose that that the tamper resistant encasement comprises an epoxy having a signature embedded therein.

However, Force et al. disclose that various encryption schemes have been proposed, such as where a user creates and **authenticates a secure digital signature**, which is very difficult to forge and thus equally difficult to repudiate (col. 4, lines 16-19). Force et al. does not explicitly teach that the encasement comprises an epoxy.

However, Schwenck et al. disclose the glass sheets 30 and 32 are in this example about [fraction (3/1000)] of an inch thick and face the polymer matrix body 16, with the glass and polymer matrix in intimate face to face contact. The body 16 is made of a black epoxy polymer material 34 such as may be commonly used in the electronics industry as an adhesive for electronic components. The matrix material 34 of the body 16 carries a chemical marker or signature: a substance present, often added specifically, to aid recognition of the matrix material in tests (¶[0056]).

Schwenck et al. further disclose the PCI card 10 of FIGS. 1 and 3 may be as previously described with a glass sheet as its outer surface, or it may be as shown in dotted outline in FIG. 3 and may have an outer shell or layer 38 of encapsulant matrix

material, **such as epoxy resin matrix, probably with a chemical signature marker(s)** (¶[0064])

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Albertshofer to include the feature of Schwenck et al. in order to provide the user the advantage of using an encasement of epoxy which is a more durable, inexpensive, and tougher encasement.

4. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albertshofer (US Patent Number 6,230,081), in view of Van De Pavert (Patent Number 5,914,471), as applied to claim 1 above, and further in view of Davis (Patent Number 5,844,986).

As per claim 9, Albertshofer does not disclose that the processor comprises a cryptographic coprocessor.

However, Davis et al. disclose that a *cryptographic coprocessor containing the BIOS memory device performs authentication and validation on the BIOS upgrade based on a public/private key protocol wherein the authentication is performed by verifying the digital signature embedded in the BIOS upgrade* (abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Albertshofer to include the feature of Davis et al. in order to prevent an attacker from trying to corrupt the BIOS contents (Davis: col. 2, lines 1-7).

5. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albertshofer (US Patent Number 6,230,081), in view of Van De Pavert (Patent Number 5,914,471), as applied to claim 1 above, and further in view of Dar et al. (US PG Pub. 2001/0039509).

As per claim 10, Albertshofer discloses the system of claim 1 as described above, but does not disclose wherein the charge comprises an insurance cost.

However, Dar et al. disclose the *data processor includes a vehicle insurance billing data processor* (¶ [0025]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Albertshofer to include the Dar et al. on order to provide a variety of uses for the data.

6. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albertshofer (US Patent Number 6,230,081), in view of Van De Pavert (Patent Number 5,914,471), as applied to claim 1 above, and further in view of Ehrman et al. (US PG Pub. 2001/0037298).

As per claim 11, Albertshofer does not disclose that the charges comprise a rental cost.

However, Ehrman et al. disclose that in some instances *the results are entered into a hand held computerized recordation device for entry into the agency computer database for calculation of the final rental charge (either while the lessee waits or as a supplement to the original charge on the initially tendered credit card).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Dar et al. to include the feature of Erhman et al. in order to effect payments for vehicle-related services including vehicle rentals (Erhman et al.;¶ [0002]).

7. Claims 16, 21 and 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dar et al. (US PG Pub. 2001/00395090), in view of Van De Pavert.

As per claims 16 and 23, Dar et al. disclose a system for managing usage information collected on a remote apparatus, comprising:

a central server for receiving information from the remote apparatus, and processing the information to obtain a usage payment (¶ [0039]);

a local data processing system installed on the remote apparatus (¶ [0038]), having:

a monitoring system for gathering usage data from the remote apparatus (¶ [0125]) { without requiring any intervention by the driver, a parking communicator 104, receiving a location input from GPS receiver 102, transmits a message in a wireless manner to a central unit 106, which in turn provides data used for effecting payment for parking};

a processor for managing the usage data (¶ [0039]) {at least one data processor which provides a billing data output in respect of a vehicle-related service} a

communications system for communicating information from the processor to the central server (¶ [0038],[0125]).

Dar et al. does not disclose a security system which includes an encryption system.

However, Ando et al. disclose that the *on-board device must include a security system for protecting monetary data stored therein and ensuring legitimate communication with the stationary device* (col. 1, lines 26-30). Ando et al. further disclose that *the illegitimate opening of the on-line device can be detected by sensing the removal of crews fastening a circuit board to a case of the on-board device* (col. 2, lines 7-9). Ando et al. further *disclose that the switch is connected to a processor of the on-board device to detect the removal of the screws* (col. 2, lines 11-13). Ando et al. still further disclose that *Detectors 5 and 7 detect a vehicle and set a timing of communication between the on-board device and the stationary device. Gate entrance detector 9 and gate exit detector 10 set a timing of opening and closing the gate* (col. 3, lines 30-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to. modify the invention of Dar et al. to include the security system feature of Ando et al. in order to protect the monetary data stored therein the sensor (Ando et al.; col. 1, lines 26-30).

As per claims 21 and 24, Dar et al. disclose the system of claim 20, wherein the usage payment comprises an insurance payment (¶ [0025]) {the data processor includes a vehicle insurance billing data processor}.

8. Claims 17 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dar et al. (US PG Pub. 2001/0039509), in view of Van De Pavert as applied to claim 16 above, and further in view of Ando et al. (Patent Number 5,955,970).

As per claims 17 and 19-20, Dar et al. does not disclose a security system comprising a tamper resistant encasement that encases at least one component of the local data processing system; a central server for receiving the processed usage data and securing a usage payment; and the security system comprising an encryption system for encrypting usage data transmitted between the sensor and the processor.

However, Ando et al. disclose that the on-board device must include a security system for protecting monetary data stored therein and ensuring legitimate communication with the stationary device (col. 1, lines 26-30). Ando et al. further disclose that the illegitimate opening of the on-line device can be detected by sensing the removal of crews fastening a circuit board to a case of the on-board device (col. 2, lines 7-9). Ando et al. still further disclose that the switch is connected to a processor of the on- board device to detect the removal of the screws (col. 2, lines 11-13). Ando et al. still further disclose the electronic toll collection system includes a stationary electronic device installed in a toll gate and an on-board electronic device mounted on a Vehicle, wherein the toll is automatically and electrically collected through wireless communication between the on-

board electronic device and the stationary electronic device; and the data to be used in the system including monetary record have to be put under security protection (col. 1, lines 49-56). Ando et al. still further disclose that Detectors 5 and 7 detect a vehicle and set a timing of Communication between the on-board device and the stationary device. Gate entrance detector 9 and gate exit detector 10 set a timing of opening and closing the gate (col. 3, lines 30-45).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Dar et al. to include the security system feature of Ando et al. in order to protect the monetary data stored therein the sensor (Ando et al.; col. 1, lines 26-30).

9. Claim 22 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dar et al. (US PG Pub. 2001/0039509), in view of Van De Pavert, in further view of Ando et al. (Patent Number 5,955,970), still in further view of Ehrman et al. (US PG Pub. 2001/0037298).

As per claim 22, Dar et al. disclose that there is also a vehicle-related fee payment system including at least one data processor which provides a billing data output in respect of a vehicle-related use fee which is dependent on the time during which the vehicle is being operated (¶ [0068]).

Dar et al. does not disclose that the charges comprise a rental cost.

However, Ehrman et al. disclose that in some instances the results are entered into a hand held computerized recordation device for entry into the agency computer database

for calculation of the final rental charge (either while the lessee waits or as a supplement to the original charge on the initially tendered credit card).

Therefore. it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Dar et al. to include the feature of Erhman et al. in order to effect payments for vehicle-related services including vehicle rentals (¶ [0002]).

As per claim 25, Dar et al. disclose the system of claim 23 as described above, but does not disclose that the usage payment comprises a rental fee.

However, Erhman et al. disclose that the customer enters a selected vehicle, punches in the prompted rental (e.g., rental duration, fuel option, insurance coverage option, return option, etc.) and identification information and, when instructed, swipes a credit Card through the reader to activate the system, with transmission of all the information to the central billing and maintenance data base which transmits details to the checkout gate, where a rental agreement is printed out, when the vehicle arrives at the gate (¶ [0031]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Dar et al. to include the payment feature of Erhman et al. in order to include in-vehicle check out and payment device operatively linkable to the transmitting sensor of the vehicle (Erhman, abstract).

11. Claims 34-35 and 37-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albertshofer (US Patent Number 6,230,081), in view of Van De Pavert, as applied to claim 33 above, and further in view of Dar et al. (US PG Pub. 2001/0039509), in further view of Shimizu et al. (US PG Pub. 2002/0111822).

As per claims 34-35, Albertshofer discloses the method of claim 33 as described above, but does not expressly disclose obtaining an electric payment based on the charge; and wherein the charge is an insurance cost.

However, Dar et al. disclose that the data processor includes a Vehicle insurance billing data processor cost (¶ [0012],[0025],[0045]). Dar et al. does not expressly disclose obtaining an electric payment.

Shimizu et al. disclose that and IC card might be used to subtract the beneficiary fee or add the provider compensation shown in FIG. 60 through FIG. 65; and if employed to subtract beneficiary fees, it would function in the same way as a prepaid card and to add provider compensation, it would be used like a debit card (¶ [0283]). Shimizu et al. further disclose that if memory medium 5720 could also be used for general purchases (i.e., to pay for other transactions), its utility would be enhanced. If the memory medium does not have the capability of being used to pay for general purchases, it should still be able to be credited or debited in an ATM machine by accessing the information mediator's account and adding or subtracting the amount recorded on the card (¶ [0283]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Albertshofer to include the

feature of Van De Pavert, Dar et al. and Shimizu et al. in order to provide the convenience of credit card payments.

As per claims 37-38, Albertshofer disclose the method of claim 33 as described above, but does not expressly disclose wherein the usage data is encrypted prior to being communicated to the processor; and Albertshofer does not further disclose wherein the charge is encrypted prior to being communicated to the server.

However, Shimizu et al. disclose that identity verification, then, is executed as preprocessing (setup) before data can be exchanged with the mediator. In other words, the mediator issues validation (data) 2701 to the machine or device to which it is connected via a network before the contract is in effect and based on these validation data, it can recognize which machine or device is communicating with it in the future wherein validation data 2701 may consist of a recognition code, a string in machine code used to recognize a machine or device, or they may be a cryptographic key or some other encrypted code (¶ [0207]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Albertshofer, to include the features of Van De Pavert, Dar et al. and Shimizu et al. in order to provide a more secure transfer of information.

(10) Response to Argument

Independent Claim 1:

1. Appellant's first argument appearing on Page 7 of the appeal brief, is that with respect to claim 1, Albertshofer and Van De Pavert do not disclose or suggest, inter alia, "a security system including an encryption system encrypting usage data transmitted between the sensor and the process". Specifically, the Appellant argues that *"in Van De Pavert, the communication of card data is between a card and a secure module 3 of a card operated device (FIG.2" and "neither the card nor the secure module 3 of Van De Pavert gathers usage data from a remote apparatus because neither is a sensor to gather usage of the telephone, e.g. a timer).*

In response to Appellant's argument, the examiner asserts that Van De Pavert discloses an invention which relates to the secure storage of cost data in counters of public telephone sets of the type where a caller pays by means of a card, such as a so-called ***"chip" card and relates to recording usage data in general and cost data in particular for machines through which the purchaser pays by means of a card, such as, e.g., vending machines for sweets or for soft drinks, certain types of parking meters and stamp vending machines wherein the term "card" should be taken to refer to any type of card (or equivalent of a card) which enables the user to make use of the machine in question***. Van De Pavert further disclose that here, the card advantageously and illustratively comprises a microprocessor 50 for processing data; memory 40 having a random access memory (RAM) 47 for temporarily storing data, such as usage data; and, optionally, ***cryptographic circuitry (54) for***

performing cryptographic operations, e.g., encryption and decryption (col. 15, line 2-18; FIG. 2 [1] is sensor and [2] is the processor; FIG. 3D [metering pulses]; FIG. 4).

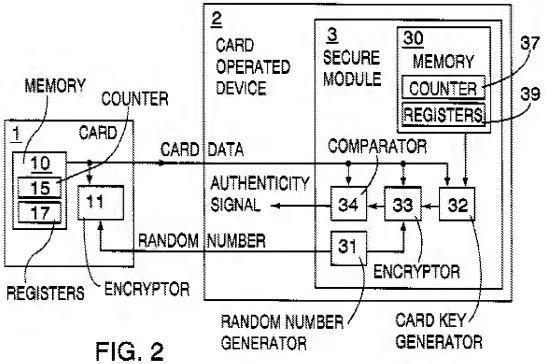

FIG. 2

In response to Applicant's argument, that in regards to independent claim 1, *"neither the card nor the secure module 3 of Van De Pavert gathers usage data from a remote apparatus because neither is a sensor to gather usage of a telephone, e.g. a timer,* the Examiner asserts that Van De Pavert discloses ***"in particular and in response to the receipt of a first metering pulse, operation c occurs to process that pulse by reducing the balance stored on the card and then transmitting an updated reduced balance back to the phone. Specifically, upon the occurrence of the metering pulse, block 150, executing within the phone, generates a decrease***

code and, as symbolized by line 151, sends that code to the card. *This decrease code instructs the card to reduce the current balance stored therein either by a given amount (i.e., here "first payment data") supplied with the code (such as, e.g., the price of an item being purchased), which could occur where a payment card similar to card 1 is used to purchase separate items of potentially differing amounts, or by a predefined fixed amount, i.e., a fixed unit, as in the case for a telephone call"* (col. 9, lines 43-56; FIG. 3D [metering pulses]).

The Appellant further argues on page 8 of the appeal brief that "cryptographic circuitry 54 does not encrypt usage data between a sensor that gathers usage data and a processor".

In response to Applicant's argument that *"cryptographic circuitry 54 does not encrypt usage data transmitted between a sensor that gathers usage data and a processor",* the Examiner asserts that Van De Pavert discloses ***cryptographically encoding said first authorization code*** (see claims 24 and 27); and an invention which relates to the secure storage of cost data in counters of public telephone sets of the type where a caller pays by means of a card, such as a so-called "chip" card and relates to recording usage data in general and cost data in particular for machines through which the purchaser pays by means of a card, such as, e.g., vending machines for sweets or for soft drinks, certain types of parking meters and stamp vending machines wherein the term "card" should be taken to refer to any type of card (or equivalent of a card) which enables the user to make use of the machine in question. Van De Pavert further disclose that here, the card advantageously and illustratively

comprises a microprocessor 50 for processing data; memory 40 having a random access memory (RAM) 47 for temporarily storing data, such as usage data; and, optionally, cryptographic circuitry (54) for performing cryptographic operations, e.g., encryption and decryption (col. 15, line 2-18; FIG. 2 [1] is sensor and [2] is the processor; FIG. 3D [metering pulses]).

2. The Appellant further argues that "in the verification procedure of Van De Pavert, a card balance is not a usage data because a use of the card has not taken place" and "that Van De Pavert expressly discloses that this procedure (including encryption) will not take place after each successive adjusting".

In response to Appellant's argument, the Examiner would like to direct that Appellant's attention to Van De Pavert's disclosure on column 8, lines 5-8. It appears that the Appellant has failed include the entire recitation of Van De Pavert, specifically, "the verification procedure…will not take place after each successive adjusting of a card balance ***during a single transaction".***

Independent Claim 33:

3. The Appellant argues that in regards to claims 1 and 33, "the card of Van De Pavert can only be used by insertion into a card operated device, and therefore there can be no encryption of usage data from a remote sensor" and Albertshofer and Van De Pavert do not disclose or suggest, inter alia, "communicating the usage data to a

processor located on a remote apparatus; and calculating a charge on the processor based on a usage data".

The Examiner asserts that Albertshofer discloses configured on the vehicle is a control unit comprising at least one first control logic for processing and displaying the vehicle travel data and a second control logic for processing and displaying further information on a graphic display arranged on the vehicle (col. 1, lines 35-39). Albertshofer further discloses a "certain credit amount is stored on the chip card as is usual for a telephone card. When the equipment item is used the validity of this card is checked and subsequently in usage of the equipment item the corresponding usage data such as e.g. duration and *intensity of use deducted from the chip card"; and* once the credit amount stored on the chip card has been exhausted the equipment item can no longer be put into operation thereby and the chip card needs to be revalidated by the equipment provider (col. 5, lines 43-52). Lastly, Albertshofer discloses also possible are ***combination cards which update the set of data in the equipment item as well as enable use of the equipment item*** (col. 6, lines 14-16).

4. The Appellant further argues on page 9 of the appeal brief that "Albertshofer clearly reveals that the billing data id provided by the base station that is not located on the vehicle".

In response to Appellant's argument, the Examiner notes that Albertshofer discloses in addition or as an alternative thereto, accounting data may also be generated right away from this usage data which is then stored on a separate location

on the chip card or added to already existing amounts or deducted from an existing total (col. 4, lines 57-61).

5. The Appellant further argues on page 10 of the appeal brief that "the office has not explained why Van De Pavert applies to claim 33.

In response to Applicant's arguments, the Examiner would like to direct the Appellant's to all the reasons stated above for claim 1.

Dependent Claims 2, 8, and 12-13:

6. Appellant's arguments appearing on Page 10 of the appeal brief, is "claims 2, 8, and 13-14 are allowable for reasons stated above, as well as their own.

In response to Appellant's argument, the Examiner respectfully disagrees for all the reason stated above for claim 1.

Dependent Claims 2, 8, and 12-13

7. Appellant's arguments appearing on Page 11 of the appeal brief is that in regards to claim 12, while the claim was rejected, there was no mention in the body why it was rejected and also the Appellant argues that claim 12 is allowable over the prior art.

In response to Appellant's argument, the Examiner notes that Albertshofer discloses chip card based accounting systems for driven machines, especially golf carts (see abstract). Furthermore, the Examiner cited areas in Albertshofer disclosing use of a vehicle. Therefore, claim 12 is also rejected for the reason stated as well as, for all the reason stated above for claim 1.

Dependent Claim 36:

8. Appellant's arguments appearing on Page 11 of the appeal brief, is "claim 36 is allowable for reasons stated above for claim 33, as well as for their own additional features.

In response to Appellant's argument, the Examiner respectfully disagrees for all the reason stated above for claim 33.

Dependent Claims 3-5 and 15:

9. Appellant's arguments appearing on Page 11 of the appeal brief is that in regards to claims 3-5 and 15, is that Ando does not overcome the deficiencies of Albertshofer and Van De Pavert because Ando does not encrypt usage data between the sensor that gathers the usage data and the processor; and moreover, Ando fails to show a tamper resistant encasement.

In response to the Appellant's argument, the Examiner asserts that Ando et al. disclose that ***the on-board device must include a security system for protecting monetary data stored therein and ensuring legitimate communication with the stationary device*** (col. 1, lines 26-30). Ando et al. further disclose that *the illegitimate opening of the on-line device can be detected by sensing the removal of crews fastening a circuit board to a case of the on-board* device. (col. 2, lines 7-9) The Examiner interprets this to mean a tamper resistant encasement). Ando et al. still further disclose that *the switch is connected to a processor of the on-board device to*

detect the removal of the screws (col. 2, lines 11-13). Ando et al. further discloses that *Detectors 5 and 7 detect a vehicle and set a timing of communication between the on-board device and the stationary device. Gate entrance detector 9 and gate exit detector 10 set a timing of opening and closing the gate* (col. 3, lines 30-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Albertshofer to include the security system feature of Van De Pavert and Ando et al. in order to protect the monetary data stored therein the sensor (Ando et al.; col. 1, lines 26-30).

Dependent Claim 6:

The Appellant argues on pages 11-12 of the appeal brief that in regards to claim 6, Force does not overcome, the above deficiencies of Albertshofer and Van De Pavert because Force does not encrypt usage data transmitted between the sensor that gathers the usage data and the processor and Force fails to show a tamper resistant encasement comprising an epoxy signature embedded therein.

In response to the Appellant's arguments, the Examiner notes that Schwenck et al. disclose the glass sheets 30 and 32 are in this example about [fraction (3/1000)] of an inch thick and face the polymer matrix body 16, with the glass and polymer matrix in intimate face to face contact. ***The body 16 is made of a black epoxy polymer material 34 such as may be commonly used in the electronics industry as an adhesive for electronic components***. ***The matrix material 34 of the body 16 carries a chemical marker or signature***: a substance present, often added

specifically, to aid recognition of the matrix material in tests (¶[0056]). Schwenck et al. further disclose the PCI card 10 of FIGS. 1 and 3 may be as previously described with a glass sheet as its outer surface, or it may be as shown in dotted outline in FIG. 3 and may have an outer shell or layer 38 of ***encapsulant matrix material, such as epoxy resin matrix, probably with a chemical signature marker(s)*** (¶ [0064]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Albertshofer to include the feature of Schwenck et al. in order to provide the user the advantage of using an encasement of epoxy which is a more durable, inexpensive, and tougher encasement.

Dependent Claim 9:

10. Appellant's arguments appearing on Page 12 of the appeal brief, is "claim 10 is allowable for reasons stated above for claim 1, as well as for their own additional features.

In response to Appellant's argument, the Examiner respectfully disagrees for all the reason stated above for claim 1.

Dependent Claim 10:

11. Appellant's arguments appearing on Page 12 of the appeal brief, is "claim 11 is allowable for reasons stated above for claim 1, as well as for their own additional features.

In response to Appellant's argument, the Examiner respectfully disagrees for all the reason stated above for claim 1.

Dependent Claim 11:

12. Appellant's arguments appearing on Page 12 of the appeal brief, is "claim 11 is allowable for reasons stated above for claim 1, as well as for their own additional features.

In response to Appellant's argument, the Examiner respectfully disagrees for all the reason stated above for claim 1.

Independent Claims 16 and 23:

13. The Appellant argues on page 13 of the appeal brief that in regards to claims 16, 21, and 23-24, that if the Office is combining Ando with Dar, Dar does not disclose or suggest, inter alia, "a local data processing system for gathering data, communicating the usage data to a processor located on the remote apparatus; and calculating a charge on the processor based on the usage data. The Appellant further argues that Ando does not overcome, inter alia, this deficiency of Dar. Ando does not encrypt usage data transmitted between the sensor that gathers the usage data and the processor, rather Ando encrypts monetary data used for paying tolls.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a local data processing system for gathering data, communicating the usage data

to a processor located on the remote apparatus; and calculating a charge on the processor based on the usage data) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Moreover, Ando et al. discloses that ***the on-board device must include a security system for protecting monetary data stored therein and ensuring legitimate communication with the stationary device*** (col. 1, lines 26-30). Ando et al. further disclose that *the illegitimate opening of the on-line device can be detected by sensing the removal of crews fastening a circuit board to a case of the on-board* device. (col. 2, lines 7-9) The Examiner interprets this to mean a tamper resistant encasement). Ando et al. still further disclose that *the switch is connected to a processor of the on-board device to detect the removal of the screws* (col. 2, lines 11-13). Ando et al. further discloses that *Detectors 5 and 7 detect a vehicle and set a timing of communication between the on-board device and the stationary device. Gate entrance detector 9 and gate exit detector 10 set a timing of opening and closing the gate* (col. 3, lines 30-45).

.

14. The Appellant further argues on page 14 of the appeal brief that claims 16 and 23 require a local processor, thus requiring that the processing be done locally and not at a centralized unit" and therefore Dar in view of Ando does not render claim 15 obvious.

In response to the Applicant's argument, the Examiner asserts that in regards to claim 16, it is noted that the features upon which applicant relies (the processing is done locally and not at a centralized unit) is not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Dependent Claims 21 and 24:

15. Appellant's arguments appearing on Page 13 of the appeal brief, is "claims 21 and 24 are allowable for reasons stated above for claim 16.

In response to Appellant's argument, the Examiner respectfully disagrees for all the reason stated above for claim 16.

Dependent Claims 17 and 19-20:

16. The Appellant argues on page 14 of the appeal brief that in regards to claims 17 and 19-20, the Office is combining Dar and Ando; and these claims are allowable for same reasons applied to claim 16. The Appellant further argues that Ando fails to disclose a tamper resistant encasement.

In response to Appellant's arguments, that in regards to claim 17, Ando fails to disclose a tamper resistant encasement, the Examiner notes that Ando et al. disclose that the on-board device must include a security system for protecting monetary data stored therein and ensuring legitimate communication with the stationary device (col. 1,

lines 26-30). Ando et al. further disclose that the illegitimate opening of the on-line device can be detected by sensing the removal of crews fastening a circuit board to a case of the on-board device (col. 2, lines 7-9). Ando et al. still further disclose that the switch is connected to a processor of the on- board device to detect the removal of the screws (col. 2, lines 11-13). Ando et al. still further disclose that Detectors 5 and 7 detect a vehicle and set a timing of Communication between the on-board device and the stationary device. Gate entrance detector 9 and gate exit detector 10 set a timing of opening and closing the gate (col. 3, lines 30-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Dar et al. to include the security system feature of Ando et al. in order to protect the monetary data stored therein the sensor (Ando et al.; col. 1, lines 26-30).

Dependent Claims 22 and 25:

17. The Appellant agues on page 15 of the appeal brief that claims 22 and 25 are allowable for same reasons stated above for claim 17.

In response to the Appellant's argument, the Examiner respectfully disagrees for all the reasons stated above for claims 17 and 19-20.

Dependent Claims 34-35 and 37-38:

18. The Appellant agues on page 15 of the appeal brief that claims 34-35 and 37-38 are allowable in view of claim 33.

In response to the Appellant's argument, the Examiner respectfully disagrees for all the reasons stated above for claim 33.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/FREDA A. NELSON/

Examiner, Art Unit 3628

Conferees:

John Hayes, SPE 3628

/John W Hayes/
Supervisory Patent Examiner, Art Unit 3628

Vincent Millin/vm/
Appeals Practice Specialist